Document Number 3

Entry 3 of 7 File: USPT Aug 31, 1999

DOCUMENT-IDENTIFIER: US 5944823 A
TITLE: Outside access to computer resources through a firewall

BSPR:
Upon receiving the request, the inside tunneling application also may be required to verify that the request is to a currently valid trusted socket and disallow the request if it is not. If the request is to a currently valid trusted socket, the inside tunneling application generates (or "spawns") an inside process associated with the request. Then the inside tunneling application: (a) generates connections between the inside resource associated with the port and host identity of the "requested" trusted socket entry and the inside interface server; and (b) communicating over the control connection with the outside tunneling application and a computer controlling the firewall itself, generates a connection through the firewall between the tasks generated/spawned on both the inside and outside interface servers. The connections generated/spawned by the inside and outside tunneling applications are separate from the control connection, and useful to carry data (usually in packet format defined by the trusted socket protocol) bidirectionally between the outside object that originated the request and the inside object targeted by the request.

CCOR:
713/201

CCXR:
380/25

WEST

Help | Logout

Main Menu | Search Form | Posting Counts | Show S Numbers | Edit S Numbers

Search Results -

Terms	Documents
l8 and control$4 near1 firewall	7

Database: US Patents Full-Text Database

Refine Search: `l8 and control$4 near1 firewall`

Search History

DB Name	Query	Hit Count	Set Name
USPT	l8 and control$4 near1 firewall	7	L23
USPT	l8 and control$4 near3 firewall	22	L22
USPT	l20 and control$4 near3 firewall	0	L21
USPT	l17 and detect$3 near1 time	7	L20
USPT	l17 and detect$3 near2 time	13	L19
USPT	l17 and detect$3 near2 overtime	0	L18
USPT	l14 and security	68	L17
USPT	l15 and control$4 near1 device	2	L16
USPT	l14 and over near1 time	17	L15
USPT	l8 and detect$3 near1 packet$	214	L14
USPT	l10 and detect$3 near3 packet$	0	L13
USPT	l10 and detecting near3 packet$	0	L12
USPT	l10 and detecting near3 pattern$	0	L11
USPT	l8 and control$4 near3 firewall	22	L10
USPT	l8 and simultaneously near1 control$4 near3 firewall	0	L9
USPT	l5 or l6 or l7	81390	L8
USPT	(340/$).ccls.	71599	L7
USPT	(380/$).ccls.	5495	L6
USPT	(713/$).ccls.	6227	L5

USPT	(713/$).ccls.	6227	L5
USPT	l1 and controller near3 device	2	L4
USPT	l1 and controller near3 device near3 control$4 near2 firewall	0	L3
USPT	l1 and controller near1 device near1 control$4 near2 firewall	0	L2
USPT	security near3 firewall	103	L1

Document Number 6

Entry 6 of 7 File: USPT Apr 20, 1999

DOCUMENT-IDENTIFIER: US 5896499 A
TITLE: Embedded security processor

DEPR:
User authentication information 140, initial firewall configuration 150, and firewall monitoring program 160 are all stored in main memory 130. User authentication program 140, initial firewall configuration 150, and firewall monitoring program 160 are all examples of firewall control programs and are executed by main processor 110 to control the activity of embedded security processor 173.

CLPR:
9. The apparatus of claim 8 wherein the firewall control program comprises a user authentication program.

CLPR:
10. The apparatus of claim 8 wherein the firewall control program comprises an initial firewall configuration program.

CLPR:
12. The apparatus of claim 8 wherein the firewall control program comprises a firewall monitoring program.

CLPR:
16. The method of claim 15 wherein the at least one firewall control program is a user authentication program.

CLPR:
17. The method of claim 15 wherein the at least one firewall control program is an initial firewall configuration program.

CLPR:
18. The method of claim 15 wherein the at least one firewall control program is a firewall monitoring program.

CLPR:
32. The method of claim 31 wherein the at least one firewall control program is a user authentication program.

CLPR:
33. The method of claim 31 wherein the at least one firewall control program is an initial firewall configuration program.

CLPR:
34. The method of claim 32 wherein the at least one firewall control program is a firewall monitoring program.

CLPV:
a memory coupled to the processor, the memory containing at least one firewall control program, the processor executing the at least one firewall control program to control access between the first and second networks.

CLPV:
providing a memory coupled to the processor, the memory containing at least one firewall control program; and

CLPV:
the processor executing the at least one firewall control program to control access between the first and second networks.

CLPV:
the processor disabling the embedded security processor if the at least one firewall control program detects an activity by the embedded security processor designated as an undesired activity by the at least one firewall control program.

CLPV:
the processor disabling the embedded security processor if the at least one firewall control program detects an unauthorized attempt by one of the first and second networks to access the other network.

CLPV:
providing a memory coupled to the processor, the memory containing at least one firewall control program; and

CLPV:
the processor executing the at least one firewall control program to control access between the first and second networks.

CLPV:
the processor disabling the embedded security processor if the at least one firewall control program detects an activity by the embedded security processor designated as an undesired activity by the at least one firewall control program.

CLPV:
the processor disabling the embedded security processor if the at least one firewall control program detects an unauthorized attempt by one of the first and second networks to access the other network.

CCOR:
713/201